噩 4 (12) (19)日本国格許庁(JP)

€ 年少 盂 蜌

(11)特許出顧公開番号

	101
	-
14871A)	(000)
-148	Wettern High Control
(P2001-	1
(P2	41
	D 83/7/67/
	(4)

特別2001-14871 (P2001-14871A)	197 198 19	G11C 17/00 601P	310 G06F 12/14 310B 5B025	310F	
	12000000000000000000000000000000000000		3 1 0	•	
		16/02	12/14		

G06F

(51) Int CL. G11C 審査請求 未請求 請求項の数9 〇L (全8 頁)

8258 (71) 出版人 00000378	株式会社東芝	9日(1999.6.29) 神奈川県川崎市幸区堀川町72番地	(72)発明者 葛西 央倫	神奈川県川崎市幸区小向東芝町1番地 株	式会社東芝マイクロエレクトロニクスセン	₹1-¢	(72)発明者 西村 望	神奈川県川崎市幸区小向東芝町1番地 株	式会社東芝マイクロエレクトロニクスセン	ター内	(74)代理人 100058479	中理士 竹江 民彦 (外6名)	最株別に扱く
特原 平11-183228		平成11年6月29日(1999.6.29)											
(21) 出數器母	1	(22) 州町日											

不揮発性半導体配筒装置 (54) [発財の名称]

機能の解除方法が知られた場合にも、保持データが捏造 ・确洩されるのを防止できるようにすることを最も主要 【熌웶】本発明は、セキュリティ機能およびプロテクト 機能を備えるフラッシュメモリにおいて、セキュリティ な健康とする。

も、保持データが外部に踊れるのを防ぐ構成となってい タの破壊を防止するために、プロテクト情報/セキュリ ティ情報記憶回路内のプロテクト用セルによってプロテ 機能の解除が指示されたとする。すると、プロテクト用 セルによるプロテクト情報の設定を無視して、各プロッ 後、セキュリティ情報の設定を解除することで、たとえ クト情報が設定されている状態において、セキュリティ [解決手段] たとえば、誤審き込みなどによる保持デー ク内のすべての保持データを強制的に消去する。この 第三者によってセキュリティ機能が解除されたとして

プロテクト価値 製造した当治 < ST15 -S114 プロチクト用セル12a~12cオフ セキュリティ周セル12dオフ セキュリティ解除 BLK115単M BLK11C当外 BLK11a激素 ST11-STIB ST12

【請求項1】 保持データを記憶する、書き換え可能型 [特許請求の範囲] のメモリ手段と、

禁止するための書き換え禁止併報を設定することが可能 このメモリ手段における、前配保持データの審き換えを

前記メモリ手段からの、前記保持データの読み出しを禁 止するための読み出し禁止情報を設定することが可能な な書き換え禁止手段と、

この説み出し禁止手段での前記説み出し禁止情報の設定 による説み出し禁止状態を解除する際、前記書き換え禁 前記メモリ手段における前記保持データを消去する消去 手段とを具備したことを特徴とする不繟発性半導体記憶 止手段での前記書き換え禁止情報の設定にかかわらず、

し禁止手段は、前記メモリ手段内に設けられることを特 手段による笛き換え禁止情報の設定が可能であることを ブロックに分割され、各エリアごとに前記書き換え禁止 【請求項3】 前記書き換え禁止手段および前記読み出 特徴とする請求項1に記載の不耀発性半導体記憶装置。 徴とする請求項1に記載の不揮発性半導体記憶装置。

る前記保持データを消去した後に、前記説み出し禁止手 [請求項4] - 前記消去手段は、前記メモリ手段におけ 段での前記読み出し禁止情報の設定を解除せしめること を特徴とする請求項1に記載の不揮発性半導体記憶装

る前記保持データを消去した後に、前記載み出し禁止手 換え禁止手段での前記書き換え禁止情報の設定を、それ ぞれを解除せしめることを特徴とする請求項1に記載の 段での前記読み出し禁止情報の設定、および、前記番き 不揮発性半導体記憶装壓。

【静水項6】 保持データを記憶する、審き換え可能型 のメモリ手段と、

禁止するための番き換え禁止情報を設定することが可能 このメモリ手段における、前記保持データの審き換えを な書き換え禁止手段と、 前記メモリ手段からの、崩記保持データの読み出しを禁 止するための読み出し禁止情報を設定することが可能な この説み出し禁止手段での前記説み出し禁止情報の設定 読み出し禁止手段と、

禁止手段での前記書き換え禁止情報の設定による書き換 による読み出し禁止状態を解除する際に、前記番き換え え禁止状態か否かを判断する判断手段と、

この判断手段によって書き換え禁止状態が判断された場 合、前記メモリ手段における前記保持データを消去する この消去手段により、前記メモリ手段における前記保持

データが消去された後に、前記読み出し禁止手段での前

【請求項2】 前記メモリ手段は、配億エリアが複数の 【精水項5】 前記消去手段は、前記メモリ手段におけ 読み出し禁止手段と、

記読み出し禁止情報の設定を解除する解除手段とを具備 したことを特徴とする不揮発性半導体配億装置。

プロックに分割され、各エリアごとに前記 き換え禁止 手段による書き換え禁止情報の設定が可能であることを 「請求項8」 前記審き換え禁止手段および前記試み出 [請求項7] 前記メモリ手段は、記憶エリアが複数の し禁止手段は、前記メモリ手段内に設けられることを特 特徴とする請求項6に記載の不揮発性半導体記憶装置。 徴とする請求項6に記載の不揮発性半導体記憶装置。

[開水項9] | 前記解除手段は、さらに、前記メモリ手 段における前記保持データが消去された後に、前記番き 換え禁止手段での前記審き換え禁止情報の設定を解除せ しめることを特徴とする請求項6に記載の不揮発性半導 体記憶装置。

[発明の詳細な説明]

[発明の咸する技協分野] この発明は、不解発性半導体 h EFPROM (Electrically Erasable Programmabl 記憶装置に関するもので、特に、セキュリティ機能およ ぴプロテクト機能を備えるフラッシュメモリ (Flais e Read Only Memory))に関するものである。 0001

[0002]

プロテクト機能)、および、保持データの能み出しを禁 止する手段(以下、セキュリティ機能)を有するものが 番き換えが可能なフラッシュメモリがあげられる。この フラッシュメモリには、保持データの程谱・環液を防ぐ [従来の技術] 周知のように、不得発性半導体記憶装置 ために、保持データの審き換えを禁止する手段(以下、 としては、ユーザによるオンボード (On-Boad)

る、プロテクト機能/セキュリティ機能の基本的概念に 【0003】以下に、従来のフラッシュメモリにおけ ついた説明する。

[0004] 図4は、従来のフラッシュメモリにおける プロテクト機能の基本概念を示すものである。

本体101とは別の、専用のフラッシュメモリ (Fuse C ell Array)からなるプロテクト情報記憶回路102内 [0005] たとえば、フラッシュメモリ本体101に ン)状態または審き換え許可(プロテク・ト,オフ)状態 を設定するためのプロテクト情報は、フラッシュメモリ 対する、保持データの書き換え禁止(プロテクト、オ に配憶されるようになっている。

は、たとえば、ステートマシン103内の、アンド回路 [0006]そして、保持データの雷き換え/消去時に 103aによる、コマンドインターフェイス104から の信号と上記プロテクト情報記憶回路102内のプロテ **クト情報とのアンド出力にしたがって、毎き込み/消去** 周御回路1036が制御されるように構成されている。

0.2内のプロテクト情報として、たとえば「1」が記憶 【0007】 すなわち、上記プロテクト情報記憶回路1

8

3

18号 (アンド川力)が「1 (許可)」となる。これによ り、ステートャシン103による、フラッシュメモリ本 上記コマンドインターフェイス104からの信号の供給 にともなって、上記アンド回路103aからの審き換え 体101に対する保持データの書き込み/消去が許可さ されて、プロテクト,オフが設定されているとすると、

【0008】 -- 方、上記プロテクト情報記憶回路102 内に「0」が記憶されて、プロテクト、オンが設定され aからの書き換え信号が「O (不可)」となる。これに ている場合には、上記コマンドインターフェイス104 からの信号の供給にかかわらず、上記アンド回路103 より、フラッシュメモリ本体101に対する保持データ の費き込み/消止が禁止される。

[0009] ブロテクト機能とは、こうしたプロテクト 保持データの書き込み/消去の許可/禁止を制御するこ とで、正規ユーザ以外の第三者による保持データの捏造 情報に応じて、フラッシュメモリ本体101に対する、 を防止するものである。

【0010】また、このようなプロテクト機能は、フラ ッシュメモリ本体の記憶エリア (アドレス領域) が複数 のブロックに分割されているフラッシュメモリにおいて は、各プロックごとにプロテクト情報を設定することが 可能とされる場合が多い。

(BLKО) 内に保持しているデータは雷き換え頻度の 【0011】たとえば、記憶エリアが複数のブロックに 分割されているフラッシュメモリ本体の、あるブロック 少ない (またに、重要な) ブログラムであり、別のブロ ック (BI.KI) 内に保持しているデータは審き換え頻 質の多いデータであるとすると、緊慢き込みなどによる し、プロック(BLK1)に対してはプロデクト情報の 牧伝が面倒(W/E時間の増加)などの理由から、プロ データ破壊がシステムの致命傷となるため、この場合、 プロック (BI.KO) に対してはプロテクト、オンと

【負012】 図5は、従来のフラッシュメモリにおける セキュリティ機能の基本概念を示すものである。 テクト、オフとするといった使用例がある。

[0013] たとえば、フラッシュメモリ本体101に 対する、保持データの読み出し禁止(セキュリティ、オ ン)状態または読み出し許可(セキュリティ、オフ)状 館を設定するためのセキュリティ情報は、フラッシュメ モリ本体101とは別の、専用のフラッシュメモリ(Fu se Cell Array)からなるセキュリティ情報記憶回路1 05内に記憶されるようになっている。

[0014] そして、保持データの読み出し時には、た とえば、デーク制御回路106内の、アンド回路106 aによる、競み出し制御回路106bからの信号と上記 セキュリティ情報記憶回路105内のセキュリティ情報 とのアンド出力にしたがって、読み出し回路107とデ ータ出力端子Dout との間の設けられたトライステート

| 0 5 内のセキュリティ情報として、たとえば「1」が ると、上記読み出し制御回路106bからの信号の供給 **11号 (アンド出力) が「1 (許可)」となる。これによ** り、上紅トライステート・バッファ108がイネーブル の、上記データ出力端子Dout を介しての読み出しが許 【0015】すなわち、上記セキュリティ情報記憶回路 記憶されて、セキュリティ,オフが設定されているとす にともなって、上記アンド回路106gからの読み出し 状態となって、上記読み出し回路107により上記フラ ッシュメモリ本体101内から読み出された保持データ パッファ108が制御されるように構成されている。

【0016】一方、上記セキュリティ情報記憶回路10 5内に「0」が記憶されて、セキュリティ,オンが故定 されている場合には、上記読み出し制御回路1065か からの説み出し信号が「0 (不可)」となる。これによ らの信号の供給にかかわらず、上記アンド回路106a がHigh-2(または、固定データ出力)の状態とな **って、フラッシュメモリ本体101からの保持データの** り、上記トライステート・パッファ108の出力.(2) 数み川しが禁止される。

で、正規ユーザ以外の第三者への保持データの漏洩を訪 【0017】セキュリティ機能とは、こうしたセキュリ の、保持データの読み出しの許可/禁止を制御すること ティ情報に応じて、フラッシュメモリ本体101から 止するものである。

【0018】また、このようなセキュリティ機能は、フ ラッシュメモリ本体の記憶エリア (全アドレス領域) に 対して、1つのセキュリティ情報を設定することが可能 とされる場合が多い。

【0019】次に、上起したプロテクト情報およびセキ ュリティ情報の設定方法について、簡単に説明する。

[0020] 図6は、プロテクト情報およびセキュリテ なお、ここでは、フラッシュメモリ本体の記憶エリアが ンド) により、専用のフラッシュメモリ201に対する 【0021】プロテクト情報およびセキュリティ情報を 設定する場合、外部トリガ(たとえば、端子情報//コマ イ情報の散定方法を説明するために示す機略図である。 複数のブロックに分割されている場合を例に説明する。 暫き換えシーケンスに入る。

【0022】そして、プロテクト情報を書き換える場合 (たとえば、フラッシュメモリ本体の記憶エリアが3つ **力端子Addより、コマンドインターフェイス202お** のプロックに分割されているとする)には、アドレス入 よび番き込み/消去回路203に供給されるブロック情 報(アドレス)をもとに、プロテクト情報記憶回路10 2内の、対象のセル102a, 102b, 102cに対 してオン/オフの設定が行われる。 【0023】また、セキュリティ情報を審き換える場合 には、端子/アドレスなどの情報にしたがって、セキュ

リティ情報記憶回路105を構成するセル102dの遊 沢が行われた後に、該セル102dに対するオン/オフ の散定が行われる。

【0024】しかしながら、このような構成のフラッシ ュメモリにおいては、セキュリティ情報を散定(セキュ **漏洩を防止できるものの、セキュリティ機能の解除方法** が知られた場合には、第三者に保持データが容易に捏造 る、セキュリティ機能の解除動作にかかる処理の流れを リティ、オン)することによって、保持データの程造・ ・漏洩される可能性があるというデメリットがあった。 [0025] 図7は、従来のフラッシュメモリにおけ 示すものである。

[0036]

[0026] たとえば、閻誓き込みなどによる保持デー て、プロテクト情報が設定(プロテクト,オン)されて いる状態において、セキュリティ機能の解除(セキュリ タの破壊を防止するために、全ブロックBI.Kについ ティ、オフ)が指示されたとする。 [0027] すると、セキュリティ情報の設定を解除す 順にチェックして、プロテクト、オフのブロックBLK 内の保持データのみ、頃次、消去する(ステップST0 合、まず、各ブロックBLKのブロテクト情報の設定を るためにセキュリティ用セルをオフにするが、この場 1~ST03),

とから構成されている。

[0028] しかる後、セキュリティ情報の散定を解除 【0029】すなわち、プロテクト情報が設定されてい ない場合には、そのブロックBLK内の保持データの消 去を行い、プロテクト情報が設定されている場合には、 そのブロックBLK内の保持データの消去を行わずに、 して(ステップST04)、一連の動作を終了する。 セキュリティ情報の設定が解除される。

場合には、保持データの内容が第三者に知られることに 果、セキュリティ機能の解除が第三者によって行われた [0030] この場合、保持データが失われないまま、 **豚保持データの読み出しが可能な状態となる。その結**

【0031】なお、保持データを認み出した後には、再 るため、プロテクト用セルをオフにして、プロテクト機 度、当該ブロックBLK内にデータを審き込む必要があ 能を解除する。 [0032] そして、当該ブロックBI.K内にデータを **むき込んだ後、必要に応じて、プロテクト情報の散定** (プロテクト、オン) が行われる。

[0033] このように、従来は、セキュリティ機能の 解除の方法が知られてしまった場合には、第三者による り、プロテクト機能/セキュリティ機能は全く意味のな 保持データの改ざん (捏造) までもが容易に可能とな いものとなるという問題があった。

[0034]

[発明が解決しようとする機題] 上記したように、従来 においては、セキュリティ機能の解除方法が知られた場

合には、第三者に保持データが容易に捏造・環復される 可能性があるという問題があった。

解除方法が知られた場合にも、保持データが捏造・環復 されるのを防止でき、保持データの機密性を飛躍的に向 [0035] そこで、この発明は、セキュリティ機能の 上させることが可能な不揮発性半導体記憶装置を提供す ることを目的としている。

情報を設定することが可能な読み出し禁止手段と、この えを禁止するための書き換え禁止情報を設定することが る説み出し禁止状態を解除する際、前記書き換え禁止手 段での前記事き換え禁止情報の設定にかかわらず、前記 [韘題を解決するための手段] 上記の目的を遵成するた と、このメモリ手段における、前記保持データの審き機 可能な蛮き換え禁止手段と、前記メモリ手段からの、前 記保持データの説み出しを禁止するための説み出し禁止 統み出し禁止手段での前記説み出し禁止情報の設定によ メモリ手段における前記保持データを消去する消去手段 めに、この発明の不揮発性半導体記憶装置にあっては、 保持データを記憶する、審き換え可能型のメモリ手段

段と、この読み出し禁止手段での前配説み出し禁止情報 の設定による統み出し禁止状態を解除する際に、前記書 記保持データが消去された後に、前記説み出し禁止手段 【0037】また、この発明の不御発性半導体記憶装置 にあっては、保持データを記憶する、審き換え可能型の メモリ手段と、このメモリ手段における、前配保持デー タの番き換えを禁止するための審き換え禁止情報を設定 することが可能な笛き換え禁止手段と、前記メモリ手段 からの、前記保持データの読み出しを禁止するための説 み出し禁止情報を設定することが可能な認み出し禁止手 き換え禁止手段での前記書き換え禁止情報の設定による 審き換え禁止状態か否かを判断する判断手段と、この判 断手段によって審き換え禁止状態が判断された場合、前 記メモリ手段における前配保持データを消去する消去手 段と、この消去手段により、前記メモリ手段における前 での前記説み出し禁止情報の数定を解除する解除手段と から構成されている。

【0038】この発明の不揮発性半導体記憶装置によれ ば、苦き後え禁止情報の設定にかかわらず、競み出し禁 止情報の設定が解除された場合には、メモリ手段におけ る保持データを消去できるようになる。これにより、た とえ第三者が競み出し禁止情報の設定を解除する方法を 知ったとしても、保持データが第三者の目に触れるのを 避けることが可能となるものである。

[発明の実施の形態] 以下、この発明の実施の形態につ いて図画を参照して説明する。

[0040] (一実施形態) 図1は、本発明の一実施形 態にかかる不揮発性半導体記憶装置の蝦略構成を、フラ 9

パシュメモリ (Flash EEPROM) を例に示す

コマンドインターフェイス13、ステートマシン(消去 トライステート・バッファ17、および、電源回路18 [0041] このフラッシュメモリは、たとえば、フラ 手段) 14、データ制御回路15、読み出し回路16、 1、プロテクト情報/セキュリティ情報記憶回路12、 ッシュメモリ本体(書き換え可能型のメモリ手段)1 を有して構成されている。

記憶するためのもので、たとえば、記憶エリア (全アド 【0042】 フラッシュメモリ本体11は保持データを レス領域) が3つのブロック (BLK) 11a, 11 b, 11cに分割されている。

【0043】ブロテクト情報/セキュリティ情報記憶回 の、上記各ブロック11a, 11b, 11cにおける保 路12は、たとえば、上記フラッシュメモリ本体11と からなり、プロテクト機能(番き換え禁止手段)として は別b、専用のフラッシュメモリ (Fuse Cell Array) 時データの番き換えを禁止するためのプロテクト情報

(書き換え禁止情報) をそれぞれ記憶するプロテクト用 セル12g,12b,12cと、セキュリティ機能(説 1 b, 11 c に対する保持データの読み出しを禁止する ためのセキュリティ情報(龍み出し禁止情報)を記憶す み出し禁止手段)としての、上記全プロック11a,1 るセキュリティ用セル12dとを有して構成されてい

ーブル信号入力端子 (/WE)、ブロック情報 (アドレ て、上記フラッシュメモリ本体11に対するデータの説 [0044] コマンドインターフェイス13は、たとえ チップイネーブル信号入力端子 (/CE) 、ライトイネ を介して、それぞれ外部より供給される情報にもとろい Aduloが、ひき込みか、消去かを判断し、上記ステート ス) 入力端子Add、および、データ入力端子 (Din) ば、アウトブットイネーブル信号人力端子 (/0E) マシン14を制御するものである。

アクト情報の設定に応じて、上記フラッシュメモリ本体 【月045】ステートマシン14は、上記コマンドイン セキュリティ情報記憶回路12内に記憶されているプロ 11に対するデータの書き込み/消去を実行するもので ターフェイス13の制御のもと、上記プロテクト情報/

[0046]また、メデートマシン14は、たとえば図 5に示したように、セキュリティ機能の解除 (セキュリ ティ、オフ)が指示された場合には、上記プロテクト情 報/セキュリティ情報記憶回路12内のプロテクト用セ ル12a~12cをチェックして、プロテクト情報の設 定により番き換え禁止(プロテクト、オン)状態かを判 断し、蓄き換え禁止状態であれば、骸プロテクト情報の 設定を無視して、上記フラッシュメモリ本体11内の金 ブロック11a~11cにおける保持データの消去を行

:

うようになっている (消去手段)。

ネーブル信号入力端子 (/CE) からの各情報と、上記 **意されているセキュリティ情報の設定とに応じて、上記** プロテクト情報/セキュリティ情報記憶回路12内に記 [0047] データ制御回路15は、上記アウトプット フラッシュメモリ本体11より読み出された保持データ の外部への出力を許可するかを決定し、上記トライステ **イネーブル信号入力端子(/OE)および上記チップイ** ート・バッファ17を制御するものである。

[0048] 読み出し回路16は、上記フラッシュメモ J本体11内の保持データを、ブロック11a~11c ごとに読み出して、上記トライステート・バッファ17 に供給するものである。

ータ制御回路15の制御にしたがって、上記読み出し回 【0049】トライステート・バッファ17は、上記デ 路16からの保持データをデータ出力増子Dout に出力 するか、または、HighーZの状態となって、その保 特データの上記データ出力端子Dout への出力を阻止 (または、固定データを出力) するものである。

[0050] 電源回路18は、動作に必要な所望の電位 を生成して、各部に供給するものである。

およびペリファイに関しては、既知の技術(徒来のフラッシュメモリと基本的に同じ)であるため、ここでの教 【0051】次に、上記した構成におけるフラッシュメ モリの動作について、簡単に説明する。なお、フラッシ ュメモリ本体11に対する保持データの番き込み/消去 明は割要する。

る、セキュリティ機能の解除動作にかかる処理の流れを [0052] 図2は、本塾明のフラッシュメモリにおけ 示すものである。

11a~11cについて、プロテクト情報が設定 (プロ タの破壊を防止するために、プロテクト情報/セキュリ 2 cにより、フラッシュメモリ本体11内の全ブロック テクト、オン)されている状態において、コマンドイン ターフェイス13に対してセキュリティ機能の解除 (セ ティ情報記憶回路12内のプロテクト用セル12a~1 [0053] たとえば、餌費き込みなどによる保持デー キュリティ、オフ)が指示されたとする。

[0054] すると、この指示がステートマシン14に ロテクト情報/セキュリティ情報記憶回路12内の、プ ロテクト用セル12a~12cのプロテクト情報の散定 を無視して、各ブロック11ョ~11 c内のすべての保 送られることにより、抜ステートマシン14は、上記プ 将データを強制的に消去する(ステップSTII~ST 13)

番き換え禁止 (プロテクト, オン) 状態が設定されてい ない、沓き換え許可 (プロテクト, オフ) 状態のプロッ ク内で保持されているデータの消去のみを行うべきとこ [0055] ここで言う、プロテクト情報の設定を無視 した消去とは、本来ならば、プロテクト用セルによって

ろ (図3参照)、たとえプロテクト用セルによって番き **後え禁止状態が設定されている場合であっても、その設** 定にかかわらず、当該ブロック内で保持されているデー タの消去を可能にすることである。

【0056】全ブロック11a~11c内のすべての保 持データを消去し終えた後においては、解除手段として の雷き込み/消去回路 (図6 参照) により、プロテクト 用セル128~12cをオフにして、ブロテクト情報の **設定を解除し、これによりプロテクト機能を解除する** (ステップST14)。

タをフラッシュメモリ本体11内に告き込む必要がある ため、使い勝手を考えた場合、保持データの消去にとも なって、プロテクト用セル12a~12cをオフにして おくのが良い (番き込みを行う際には、プロテクト用セ 【0057】正規のユーザは、新たに所将しているデー ルをオフにする必要があるため)。

[0058]また、解除手段としての書き込み/消去回 路 (図6番照) により、セキュリティ用セル12dをオ フにして、セキュリティ情報の設定を解除し、これによ りセキュリティ機能を解除して (ステップST15) 、 一連の動作を終了する。 【0059】このように、セキュリティ機能の解除が特 ト, オン) にかかわらず、フラッシュメモリ本体11内 の保持データをすべて消去した後に、セキュリティ情報 の設定を解除 (セキュリティ, オフ) するようにしてい 示された場合には、プロテクト情報の設定 (プロテク

【0060】したがって、保持データの読み出しが可能 その結果、たとえ何らかの手段によって、何者かにセキ ュリティ機能の解除力法が知られたとしても、第三者に かかわらず、セキュリティ情報の設定が解除された場合 には、フラッシュメモリ本体における保持データを消去 [0061] 上記したように、プロテクト情報の設定に な状態となった際には、既に保持データは存在しない。 よる保持データの解説または改ざんは不可能となる。 できるようにしている。

をすべて消去した後に、セキュリティ情報の設定を解除 するようにしている。これにより、たとえ何らかの手段 解説または改ざんは不可能となる。したがって、正規の 【0062】すなわち、セキュリティ機能の解除が指示 によって、何者かにセキュリティ機能の解除方法が知ら れたとしても、保持データが第三者の目に触れるのを避 けることが可能となるため、第三者による保持データの ューザ以外に、保持データが捏造・環洩されるのを防止 でき、保持データの機密性を飛躍的に向上させることが された場合には、フラッシュメモリ本体内の保持データ 可能となるものである。

【0063】特に、保持データの消去にともなって、プ ロテクト用セルをオフしてプロテクト情報の設定を解除 するようにした場合には、正規ユーザの使い勝手をも向

[0064] なお、上記したこの発明の一実施形態にお

フラッシュメモリ (Fuse Cell Array) により構成する を、たとえば、フラッシュメモリ本体とは別の、専用の えばブロテクト情報/セキュリティ情報記憶回路はフラ ようにした場合を例に説明したが、これに限らず、たと いては、プロテクト情報/セキュリティ情報記憶回路。 ッシュメモリ本体内に設けることも可能である。

【0065】また、保持データの捏造・講改を防止する 方法としては、上記した方法以外に、たとえば、プロテ クト情報が設定されている保持データが存在する場合に は、セキュリティ機能を解除できないようにするなどの が泣も考えられる。

[0066] その他、この発明の要旨を変えない範囲に おいて、種々変形実施可能なことは勿論である。 [0067]

保持データが程造・環彼されるのを防止でき、保持デー タの機密性を飛躍的に向上させることが可能な不得発性 ば、セキュリティ機能の解除方法が知られた場合にも、 [発明の効果] 以上、詳述したようにこの発明によれ 半導体記憶装置を提供できる。

【図面の簡単な説明】

【図1】この発明の一実施形態にかかる、フラッシュメ モリの優略構成を示すプロック図。

[図2] 同じく、フラッシュメモリにおける、セキュリ ティ機能の解除動作にかかる処理の流れを示すフローチ [図3] 同じく、フラッシュメモリにおける、保持デー タの消去動作にかかる処理の流れを示すフローチャー

ッシュメモリにおけるプロテクト機能の基本的概念を示 [図4] 従来技術とその問題点を説明するために、フラ ナブロック図。

[図5] 同じく、従来のフラッシュメモリにおけるセキ ュリティ機能の基本的概念を示すプロック図。

[図6] 同じく、プロテクト情報およびセキュリティ情 **報の設定方法を税明するために、フラッシュメモリの要** 部の構成を概略的に示すプロック図。

キュリティ機能の解除動作にかかる処理の流れを示すフ |図1| 同じく、従来のフラッシュメモリにおける、 ローチャート。

[作号の説明]

11…フラッシュメモリ本体

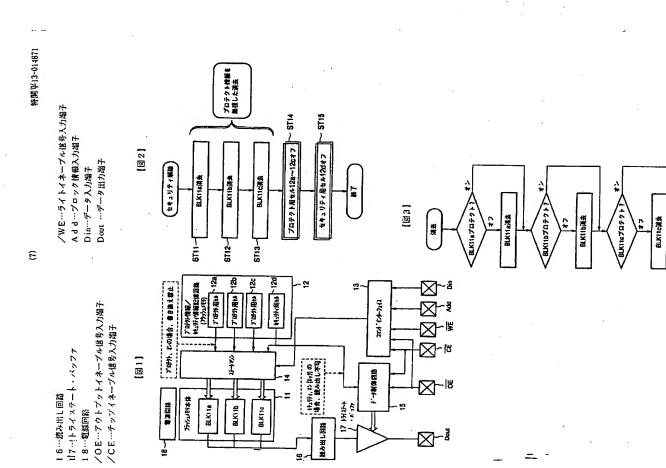
118, 116, 11c ... 707

12…ブロテクト情報/セキュリティ情報記憶回路 12a, 12b, 12c…プロテクト用セル

12 d…セキュリティ用セル

13…コマンドインターフェイス 14…ステートマシン

15…データ制御回路



ج.9

特開平13-014871

8

5

[図2]

[図4]

最か出し回路

フラッシュメモリ 本体

着き込み/消去 数像回路

フラッシュメモリ

106a 쁄.

8

日ヶ出し名物回路

호.

8

BA1Q BB03 BB05 CA12 CA16 5B025 AA03 AB01 AC01 AD08 AD14 Fターム(参考) 5B017 AA02 AA03 AA06 BA04 BA08 AE10 フロントページの検ぎ

親々出し許可となり、 保格データを知り組る 状態

セキュリティ. オフ

コマンドインターフェイス

⊠-5

⊠-₹

別去知了?

書き込み/派去四路

プロテクト、キンの BLKが選抜きれない

四人送社

全プロック について 繰り返す

¥

[図1]

2 1 F 1 MB

월~<mark></mark>Ā

[9図]

몽

セキュリティ俳優 記は国路 (フラッシュメモリ) ~105

179-7143

プロテクト情報 記述回路 (フラッシュメモリ)

Nonvolatile semiconductor memory device with security function and protect function						
Patent Number:	□ <u>US6229731</u>					
Publication date:	2001-05-08					
Inventor(s):	KASAI NOZOMI (JP); KASAI TAKAMICHI (JP)					
Applicant(s):	TOKYO SHIBAURA ELECTRIC CO (US)					
Requested Patent:	☐ <u>JP2001014871</u>					
Application Number:	US20000606146 20000629					
Priority Number(s):	JP19990183228 19990629					
IPC Classification:	G11C16/04					
EC Classification:	G11C16/22					
Equivalents:	·					
Abstract						
The invention provides a flash memory having a security function and a protect function. When the release of the security function has been instructed, all data stored in each block of a flash memory main body is forcibly erased, ignoring the setting of the protect function. After that, the security function is released, thereby enabling readout of data. This being so, even if a third person releases the security function, leakage of data to the outside can be prevented						
Data supplied from the esp@cenet database - I2						